

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

In the present Office Action, the Examiner rejected Claims 21-23, 28-34, and 37-40 as unpatentable for obviousness over Hashimoto U.S. Patent 5,931,905, in view of Paul U.S. Patent 6,052,709, and Claims 24-27, 35-36 further in view of Lillibridge U.S. Patent 6,195,698. The Claims as presented and the Applicant's argument clearly stated that the unique feature of the claimed invention is that the standard email-sending protocol is utilized to enable the email-receiving server to reject unauthorized email from a sender who is not on the user's Authorized Senders List (ASL). The Examiner cited the Paul patent as teaching that spam probes can be used to generate a list of suspected addresses of spammers sending spam email, and an standard email-sending protocol (such as MAPI) can be used to identify email sent by a suspected spammer and cause the email-receiving server to delete it. Therefore, the Applicant has amended main Claims 21, 32, and 40 to specifically recite that if the sender address of the intended email is not recognized as being on the user's ASL list, the email-receiving server sends an error message, under the common email-sending system protocol, to the email-sending server that the email will not be accepted, thereby causing the email-sending server to be blocked from sending the intended email to the email-receiving server, and deterring the spammer from sending further email to the user's address indicated to be in error by the email-sending server. The recitation added to the claims is supported in the Specification at page 5, lines 8-14, page 8, line 30, to page 9, line 1, and page 14, lines 14-31, describing the email blocking and error message sending procedure in Fig. 7B.

The function in the present invention of sending an error message that the email will not be accepted (when the sender is not authorized on the user's ASL list) and causing the email to be blocked from being sent in the first place, and also deterring the spammer from further sending email to the user's address, is a distinctly different approach and provides an important advantage not recognized in the Hashimoto and Paul patents. Both cited references repeatedly state that the email is first received, then if it is recognized as being from an unwanted sender, it is eliminated before being placed in the user's mailbox (Hashimoto) or from being stored on the receiving server (Paul). In contrast, the amended claims define the result in the present invention that the email is blocked by the error message under the email-sending protocol from ever being sent and the spammer is deterred from further spamming by receiving the error message. As evidenced in the accompanying Affidavit of Katsikas, this function and

advantageous effect was not heretofore recognized in an industry that has long sought a potent solution to the burgeoning spam problem. The solution herein was recognized only by the present inventor, and could not have been obvious to those skilled in the art at the time of the invention because no such solution had been put forward previously despite diligent efforts in the industry to solve the spam problem.

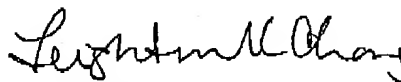
In summary, Claims 21 - 40 as amended are deemed to be patentably distinct over the cited prior art and in condition for allowance, and it is requested that a Notice of Allowance be issued therefor upon reconsideration.

This response is filed with total and independent claims after amendment numbering within the limits originally paid for with the filing fee. However, if any fees are deemed to be due for acceptance of this response, authorization is hereby given to charge our Deposit Account No. 502633.

CERTIFICATE OF MAILING:

The undersigned certifies that the foregoing is being sent by facsimile transmission to Examiner Brandon Hoffman, Group 2136, at (703) 872-9306 on
Aug. 9, 2004

Respectfully submitted,
ATTORNEYS FOR APPLICANT



Leighton K. Chong
USPTO Reg. No. 27,621
OSTRAGER CHONG & FLAHERTY (HAWAII)
841 Bishop Street, Suite 1200
Honolulu, HI 96813-3908
Tel: (808) 533-4300
(HST 6 hrs < EST)

AMENDMENT OF CLAIMS

(Claims 1-20, cancelled)

(Claim 21, amended)

21. A method for eliminating unauthorized email on a network comprising the steps of:

(a) establishing a connection on a network between an email-receiving server and an email-sending server, wherein said email-receiving server and email-sending server utilize a common email-sending system protocol to send email on the network;

(b) making accessible to the email-receiving server for each subscribing user an authorized senders list (ASL list) of email addresses of [external users] senders authorized to send email to the user,

(c) receiving at the email-receiving server, under the common email-sending system protocol, a message from the email-sending server requesting to send email which is addressed to a user deemed to receive email through the email-receiving server and which is addressed from a given sender address;

(d) causing the email-receiving server to check whether the user the intended email is addressed to is a user which receives email through the email-receiving server, and, if so, then causing the email-receiving server to check whether the sender address of the intended email is on the user's ASL list; and

(e) if the sender address of the intended email is recognized as being on the user's ASL list, causing the email-receiving server under the common email-sending system protocol to send a reply message to the email-sending server that the sending of the email to the email-receiving server will be accepted, otherwise if the sender address of the intended email is not recognized as being on the user's ASL list, causing the email-receiving server to send an error message, under the common email-sending system protocol, to the email-sending server [~~that the email-receiving server will not accept the sending of the email to the email-receiving server~~] so

as to prohibit the email-sending server from sending the intended email to the email-receiving server, whereby the sender is unable to send the unwanted email to the user and is deterred from sending further email to the user's address indicated to be in error by the email-receiving server.

(Claim 22, original)

22. A method according to Claim 21, wherein the ASL module includes an ASL database for storing ASL lists of authorized sender addresses for respective users of the email-receiving server, a spam processor module for checking the ASL lists for matches, and an ASL manager for creating, maintaining, and updating the ASL lists.

(Claim 23, original)

23. A method according to Claim 21, wherein a redirector module is provided to operate with the ASL module for receiving the message from the email-sending server requesting to send email designating the sender's address and intended recipient's address, for sending a request for validation to the spam processor module to determine whether the sender's address matches any authorized sender address maintained on the ASL list corresponding to the address of the intended recipient, for sending the reply message accepting the email from the email-sending server if a match to an authorized sender address is found, and for sending the error message not accepting the email if no match to an authorized sender address is found on the ASL list.

(Claim 24, original)

24. A method according to Claim 23, wherein a web-based messaging (WBM) module is provided to which the sender of intended email that is not accepted by the email-receiving server is redirected by the redirector module, and wherein the WBM module sends a message to the address of the sender of the non-accepted email notifying the sender to confirm with the WBM module that the sender is a legitimate sender of email to the intended recipient.

(Claim 25, original)

25. A method according to Claim 24, wherein the WBM module is a website accessible

on the network which invites the notified sender to log on and confirm that the sender is a legitimate sender of email through an interaction procedure which can only be performed by a human.

(Claim 26, original)

26. A method according to Claim 25, wherein the interaction procedure includes a display of a graphic image of a word in a non-standard font, and a prompt to the sender to enter in a word corresponding to the graphic image of the word, whereby the system can confirm that the interaction procedure is not performed by a mechanical program.

(Claim 27, original)

27. A method according to Claim 24, wherein once the sender is confirmed as a legitimate sender of email to the intended recipient user, the WBM website sends a message to the redirector module at the user's email-receiving server that the sender is confirmed as a legitimate sender by the WBM website.

(Claim 28, original)

28. A method according to Claim 22, wherein email addresses used on email sent by a user which receives email through the email-receiving server and other addresses accessed by the user on the network are captured and stored with the ASL manager for later analysis.

(Claim 29, original)

29. A method according to Claim 28, wherein the ASL manager analyzes the captured addresses using a rules processor for processing predefined address capture rules for updating the ASL lists using data from an email address source selected from the group of email address sources consisting of: received email; sent email; user inputs to email service functions on the email client; inputs from user browsing of web sites; user desktop organizer and other contact lists; and third party address program inputs.

(Claim 30, original)

30. A method according to Claim 28, wherein the ASL manager analyzes the captured

addresses using a rules processor for processing predefined analysis rules for updating the ASL lists using data from an analysis source selected from the group of analysis sources consisting of: user email log analysis; expiration date analysis; low/high email volume analysis; fuzzy logic analysis; and third party data analysis.

(Claim 31, original)

31. A method according to Claim 22, wherein the ASL manager maintains the ASL lists to designate a sender-address status for each sender address selected from the group of sender-address statuses consisting of: always authorized as a friend; authorized as a friend over a date range; authorized as a friend before an expiration date; always rejected as a spammer; rejected as a spammer matching a black list; and rejected as a spammer sent with an error message.

(Claim 32, amended)

32. A method for eliminating unauthorized email on a network comprising the steps of:

(a) establishing a connection on a network between an email-receiving server and an email-sending server, wherein said email-receiving server and email-sending server utilize a common email-sending system protocol to send email on the network;

(b) making accessible to the email-receiving server for each subscribing user an authorized senders list (ASL list) which identifies email addresses of senders not authorized to send email to the user;

(c) receiving at the email-receiving server, under the common email-sending system protocol, a message from the email-sending server requesting to send email which is addressed to a user deemed to receive email through the email-receiving server and which is addressed from a given sender address;

(d) causing the email-receiving server to check whether the user the intended email is addressed to is a user which receives email through the email-receiving server, and, if so, then causing the email-receiving server to check whether the sender address of the intended email is on the user's ASL list of ~~[external users]~~ senders not authorized to send email to the user; and

(e) if the sender address of the intended email is recognized as being on the user's

ASL list, causing the email-receiving server under the common email-sending system protocol to send a reply message to the email-sending server that the sending of the email to the email-receiving server will be accepted, otherwise if the sender address of the intended email is recognized as being not authorized on the user's ASL list, causing the email-receiving server to send an error message, under the common email-sending system protocol, to the email-sending server ~~[that the email-receiving server will not accept the sending of the email to the email-receiving server]~~ so as to prohibit the email-sending server from sending the intended email to the email-receiving server, whereby the sender is unable to send the unwanted email and is deterred from sending further email to the user's address indicated to be in error by the email-receiving server.

(Claim 33, original)

33. A method according to Claim 32, wherein the ASL module includes an ASL database for storing ASL lists of both authorized and non-authorized sender addresses for respective users of the email-receiving server, a spam processor module for checking the ASL lists for matches, and an ASL manager for creating, maintaining, and updating the ASL lists.

(Claim 34, original)

34. A method according to Claim 32, wherein a redirector module is provided to operate with the ASL module for receiving the message from the email-sending server requesting to send email designating the sender's address and intended recipient's address, for sending a request for validation to the spam processor module to determine whether the sender's address matches any authorized sender address maintained on the ASL list corresponding to the address of the intended recipient, for sending the reply message accepting the email from the email-sending server if a match to an authorized sender address is found, and for sending an error message not accepting the email if no match to an authorized sender address is found on the ASL list.

(Claim 35, original)

35. A method according to Claim 34, wherein a web-based messaging (WBM) module is provided to which the sender of intended email that is not accepted by the email-receiving server is

redirected by the redirector module, and wherein the WBM module sends a message to the address of the sender of the non-accepted email notifying the sender to confirm with the WBM module that the sender is a legitimate sender of email to the intended recipient.

(Claim 36, original)

36. A method according to Claim 35, wherein once the sender is confirmed as a legitimate sender of email to the intended recipient user, the WBM website sends a message to the redirector module at the user's email-receiving server that the sender is confirmed as a legitimate sender by the WBM website.

(Claim 37, original)

37. A method according to Claim 33, wherein email addresses used on email sent by a user which receives email through the email-receiving server and other addresses accessed by the user on the network are captured and stored with the ASL manager for later analysis, and wherein the ASL manager analyzes the captured addresses using a rules processor for processing predefined address capture rules for updating the ASL lists using data from an email address source selected from the group of email address sources consisting of: received email; sent email; user inputs to email service functions on the email client; inputs from user browsing of web sites; user desktop organizer and other contact lists; and third party address program inputs.

(Claim 38, original)

38. A method according to Claim 33, wherein email addresses used on email sent by a user which receives email through the email-receiving server and other addresses accessed by the user on the network are captured and stored with the ASL manager for later analysis, and wherein the ASL manager analyzes the captured addresses using a rules processor for processing predefined analysis rules for updating the ASL lists using data from an analysis source selected from the group of analysis sources consisting of: user email log analysis; expiration date analysis; low/high email volume analysis; fuzzy logic analysis; and third party data analysis.

(Claim 39, original)

39. A method according to Claim 33, wherein the ASL manager maintains the ASL lists to designate a sender-address status for each sender address selected from the group of sender-address statuses consisting of: always authorized as a friend; authorized as a friend over a date range; authorized as a friend before an expiration date; always rejected as a spammer; rejected as a spammer matching a black list; and rejected as a spammer sent with an error message.

(Claim 40, amended)

40. A system for eliminating unauthorized email on a network comprising:

(a) first means for establishing a connection on a network between an email-receiving server and an email-sending server, wherein said email-receiving server and email-sending server utilize a common email-sending system protocol to send email on the network;

(b) second means for making accessible to the email-receiving server for each subscribing user an authorized senders list (ASL list) for identifying which email addresses of ~~[external users]~~ senders are authorized to send email to the user;

(c) third means for receiving at the email-receiving server, under the common email-sending system protocol, a message from the email-sending server requesting to send email which is addressed to a user deemed to receive email through the email-receiving server and which is addressed from a given sender address; and

(d) fourth means for causing the email-receiving server to check whether the user the intended email is addressed to is a user which receives email through the email-receiving server, and, if so, then causing the email-receiving server to check whether the sender address of the intended email is on the user's ASL list as being authorized to send email to the user;

(e) wherein, if the sender address of the intended email is recognized as being authorized on the user's ASL list, said fourth means causing the email-receiving server to send a reply message, under the common email-sending system protocol, to the email-sending server that the sending of the email to the email-receiving server will be accepted, otherwise if the sender address of the intended email is not authorized on the user's ASL list, said fourth means causing the email-receiving server to send an error message, under the common email-sending system protocol, to the email-sending server ~~[that the email-receiving server will not accept the sending of the email to the email-receiving server]~~ so as to prohibit the email-sending server from sending the intended

email to the email-receiving server, whereby the is unable to send the unwanted email and is deterred from sending further email to the user's address indicated to be in error by the email-receiving server.